

REMARKS

Claims 1-66 are currently pending in the subject application, and are presently under consideration. Claims 1-66 are rejected. Claims 1, 2, 4, 7, 9, 10, 13, 15-17, 21, 24, 26, 28, 29, 31-33, 35, 38, 40-42, 44, 46, 48, 50, 52, 55, 57, 59, 60, and 62-66 have been amended. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Claim Objections

The claims of the present application have been objected in that the numbering of claims is not in accordance with 37 CFR 1.126, such that claims must be numbered consecutively beginning with the number next following the highest numbered claims previously presented. Accordingly, the misnumbering of claims 62-65, corrected as claims 63-66, is acknowledged and has been applied to the above listing of the claims. Additionally, claim 62 has been amended to coincide with the Examiner's correct belief that claim 62 be dependent on claim 61, and not claim 31. Withdrawal of the objection to the claims is respectfully requested.

II. Rejection of Claims 1, 7-9, 32, and 38-40 Under 35 U.S.C. §102(e)

Claims 1, 7-9, 32, and 38-40 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,308,277 to Vaeth, et al. ("Vaeth"). Claims 1, 7, 9, 32, 38, and 40 have been amended. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Amended claims 1 and 32 recite a method and a computer program, respectively, of creating a role certificate comprising transmitting a role approval form, filled out and digitally signed by the user using a personal digital signature, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. The language of amended claims 1 and 32 specifically recite that they are applicable to a role certificate, such that a user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information

which may be decrypted by a plurality of group members (see also, Specification of Present Application, page 10, line 22 through page 12, line 9). Vaeth teaches a method and system for creating and administering certificates digitally signed by a certificate authority to ensure that certified transactions are authenticated as that of a particular entity (Abstract). The types of certificates which are described by the teachings of Vaeth are those described in ANSI X9.57, "Public Key Cryptography for the Financial Services Industry, Certificate Management." (col. 1, ll. 37-41). Neither Vaeth nor the ANSI document cited in Vaeth describe a role certificate, such as described in the present application. Specifically, the invention of Vaeth does not contemplate a role certificate that is distinguishable from an individual user's digital certificate, such that a user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in amended claims 1 and 32.

In addition, amended claims 1 and 32 recite notifying the user of the availability of the role certificate. Vaeth is silent as to notification to a user as to availability of an issued certificate. Vaeth simply teaches that a copy of a certificate is delivered to the requester using secure means (col. 4, ll. 52-54). Accordingly, Vaeth does not teach notifying the user of the availability of the role certificate, as recited in claims 1 and 32, and therefore does not anticipate amended claims 1 and 32. Withdrawal of the rejection of claim 1, as well as claims 2-6 which depend therefrom, and claim 32, as well as claims 33-37 which depend therefrom, is respectfully requested.

Amended claims 7 and 38 recite a method and computer program, respectively, of using a role certificate as an organizational stamp and for organizational encryption by a plurality of role members of a group comprising signing digitally the electronic form by the role member using the role certificate and signing digitally the electronic form by the role member using a personal signature certificate, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described above with regard to amended claims 1 and 32, Vaeth

does not teach the use of a role certificate, and thus amended claims 7 and 38 should be allowable.

Additionally, in rejecting claims 7 and 38, the Office Action dated November 10, 2004, (pages 3 and 4) cites the same section of the Vaeth (col. 4, ll. 34-54) that was cited for the rejection of amended claims 1 and 32. However, amended claims 1 and 7 (as well as claims 32 and 38) each claim methods for achieving different results, such that the Office Action dated November 10, 2004, (page 3 and 4) is interpreting the teachings of Vaeth in two separate and conflicting ways. Further, amended claims 7 and 38 explicitly state that one individual (the role member) digitally signs the same electronic form using two different digital certificates. Vaeth teaches that a requestor prepares a certificate request data submission and signs it with a private key (col. 4, ll. 34-37). However, Vaeth does not teach that the requester digitally signs the document with two separate certificates, and thus does not teach a role member signing digitally the electronic form by the role member using the role certificate and signing digitally the electronic form by the role member using a personal signature certificate, as recited in amended claims 7 and 38. Accordingly, Vaeth does not anticipate amended claims 7 and 38. Withdrawal of the rejection of claim 7, as well as claims 8-10 which depend therefrom, and claim 38, as well as claims 39-41 which depend therefrom, and is respectfully requested.

Claims 8 and 39 recite retrieving a policy associated with the role certificate by the entity. Claim 8 depends from amended claim 7, and claim 39 depends from amended claim 38, and thus both should be allowable for at least the reasons described above regarding amended claims 7 and 38. Additionally, Vaeth is silent as to policies associated with a digital certificate, and therefore does not teach retrieving a policy associated with the role certificate by the entity, as recited in claims 8 and 39. Accordingly, Vaeth does not anticipate claims 8 and 39. Withdrawal of the rejection of claims 8 and 39 is respectfully requested.

Claims 9 and 40 have been amended to recite transmitting a public key portion of the role certificate by the role member to the entity, encrypting information by the entity, transmitting the information to any of the plurality of role members of the group, and decrypting the information by any of the plurality of role members of the group having the role certificate. Amended claim

9 depends from amended claim 7, and amended claim 40 depends from amended claim 38, and thus both should be allowable for at least the reasons described above regarding amended claims 7 and 38. Additionally, the amendment to claims 9 and 40 clarifies that decrypting the information can be by any of the plurality of role members of the group having the role certificate, which is not taught by Vaeth. Accordingly, Vaeth does not anticipate amended claims 9 and 40. Withdrawal of the rejection of claims 9 and 40 is respectfully requested.

For the reasons described above, claims 1, 7-9, 32, and 38-40 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 11-14, 16-22, 24, 26-28, 42-45, 48-53, 55, 57-59, and 63-66 Under 35 U.S.C. §102(e)

Claims 11-14, 16-22, 24, 26-28, 42-45, 48-53, 55, 57-59, and 63-66 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,301,658 to ("Koehler"). Claims 13, 16, 17, 21, 24, 26, 28, 42, 44, 48, 50, 52, 55, 57, 59, and 63-66 have been amended. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 11 and 42 recite a method and computer program, respectively, of replacing an expiring role certificate comprising displaying a list of roles to a user who is either a role member or a role administrator, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. Koehler teaches a method and system for efficiently authenticating digital certificates issued by an organization's authentication hierarchy (Abstract). Claims 11 and 42 recite elements that are to be performed to/for a role certificate, such that the role certificate can be utilized by a user that is a member of a group as a group stamp and for encryption of information which may be decrypted by a plurality of group members. The digital certificates taught by Koehler are user digital certificates (see, *e.g.*, col. 3, line 46; col. 3, line 62; and col. 4, line 8), which are "conventional" digital certificates (see, *e.g.*, col. 4, line 46 and col. 4, line 57 through col. 5, line 41) in the discussion of the problems solved by Koehler. Koehler does not contemplate a role certificate that can be used by a user who is either a role member or a role

administrator, such that the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claims 11 and 42.

In addition, claims 11 and 42 further recite selecting a role which is about to expire for renewal by the user, determining if the user is authorized to renew the role based upon verification of the user's personal digital signature, generating a new role certificate having a private and public key, and transmitting the new role certificate to the user. The Office Action dated November 10, 2004, (at pages 5-6 and 9) asserts that claims 11 and 42 are taught by Koehler (at col. 3, ll. 12-19 and col. 3, ll. 25-30). Koehler teaches that a certificate revocation list can be maintained that lists revoked and expired certificates, prompting authentication of a certificate against the revocation list (col. 3, ll. 12-19), and further teaches that systems may cache expiration periods for certificates, such that expired certificates are removed and new certificates are authenticated (col. 3, ll. 25-30). However, neither of these cited sections, nor any other sections of Koehler, teach selecting a role which is about to expire for renewal by the user, determining if the user is authorized to renew the role based upon verification of the user's personal digital signature, generating a new role certificate having a private and public key, and transmitting the new role certificate to the user, as recited in claims 11 and 42. Accordingly, Koehler does not anticipate claims 11 and 42. Withdrawal of the rejection of claim 11, as well as claims 12-16 which depend therefrom, and claim 42, as well as claims 43-47 which depend therefrom, is respectfully requested.

Claims 12 and 43 recite that the transmitting of the new role certificate to the user is done over an encrypted secure communications line. Claims 12 and 43 depend from claims 11 and 42, respectively, and should be allowable for at least the reasons described above with regard to claims 11 and 42. In addition, the Office Action dated November 10, 2004, (pages 6 and 9) asserts that Koehler (at col. 5, ll. 55-62) teaches claims 12 and 43. Koehler teaches that a verification server is a client process serving multiple client processes on a single machine, or serves clients distributed across a network, and that a certificate repository maintains all digital certificates issued by an authentication hierarchy in a directory (col. 5, ll. 55-62). The cited

section of Koehler has nothing to do with transmission of a new certificate, or that transmission of a new certificate is done over an encrypted secure communications line. In fact, Koehler does not teach transmitting a new certificate (a role certificate or otherwise) to a user over an encrypted secure communications line, as recited in claims 12 and 43. Accordingly, Koehler does not anticipate claims 12 and 43. Withdrawal of the rejection of claims 12 and 43 is respectfully requested.

Claims 13 and 44 have been amended for clarity and recite that prior to the transmitting of the new role certificate to the user, the new role certificate is transmitted to a certificate authority for approval, and the new role certificate is not transmitted to the user without the approval. Claims 13 and 44 depend from claims 11 and 42, respectively, and thus should be allowable for at least the reasons stated above regarding claims 11 and 42. Withdrawal of the rejection of claims 13 and 44 is respectfully requested.

Claims 16, 21, 24, 28, 52, 55, and 59 have been amended for clarity and recite that the role certificate comprises a public key, a private key, a signature algorithm ID, a validity period, extensions, and at least one policy. Claim 16 depends from claim 11, claim 21 depends from claim 17, claim 24 depends from claim 22, claim 28 depends from claim 26, claim 52 depends from claim 48, claim 55 depends from claim 53, and claim 59 depends from claim 57. Therefore, claims 16, 21, 24, 28, 52, 55, and 59 should be allowable for the same reasons as described regarding claims 11, 17, 22, 26, 48, 53, and 57, respectively. Additionally, Koehler teaches that "a typical digital certificate [has] six data fields including owner information, the owner's public key, validity period, serial number, issuer information and issuer's digital signature." (col. 4, line 66 through col. 5, line 2). Koehler also teaches that a verification cache is organized for efficient lookup of an item and is organized by owner and information type, with each cache entry storing information such as the item's timestamp, expiration data, issuer and user privileges (col. 6, ll. 5-8). However, Koehler does not teach that a certificate (role certificate or otherwise) comprises extensions and at least one policy, as recited in claims 16, 21, 24, 28, 52, 55, and 59. Accordingly, Koehler does not anticipate claims 16, 21, 24, 28, 52, 55,

and 59. Withdrawal of the rejection of claims 16, 21, 24, 28, 52, 55, and 59 is respectfully requested.

Amended claims 17 and 48 recite a method and computer program, respectively, of revoking a role certificate used as an organizational stamp and for organizational encryption by authorized members of the organization comprising transmitting a signature certificate to a registration web server by a user, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described above with regard to claims 11 and 42, Koehler does not teach the use of a role certificate, and thus amended claims 17 and 48 should be allowable.

In addition, amended claims 17 and 48 further recite transmitting a signature certificate to a registration web server by a user, authenticating by accessing a directory that the user is still a member of the organization, listing roles of which the user is a role member or a role authority, and removing the role certificate associated with the role from a directory database. The Office Action dated November 10, 2004, (at pages 6-7 and 10) cites the same sections of Koehler as those cited for the rejection of claims 11 and 42 to assert that amended claims 17 and 48 are taught by Koehler (particularly, col. 3, ll. 12-19 and col. 3, ll. 25-30). However, claims 11 and 17 (as well as claims 42 and 48) each claim methods for achieving different results, such that the Office Action dated November 10, 2004, is interpreting the teachings of Koehler in two separate and conflicting ways. Koehler does not teach, neither in the cited section nor anywhere else, transmitting a signature certificate to a registration web server by a user, authenticating by accessing a directory that the user is still a member of the organization, listing roles of which the user is a role member or a role authority, and removing the role certificate associated with the role from a directory database, as recited in amended claims 17 and 48. Accordingly, Koehler does not anticipate amended claims 17 and 48. Withdrawal of the rejection of claim 17, as well as claims 18-21 which depend therefrom, and claim 48, as well as claims 49-52 which depend therefrom, is respectfully requested.

Claims 18 and 49 recite that when the role certificate is removed from the directory database, the role associated with the role certificate remains intact on the database. Claims 18 and 49 depend from claims 17 and 48, respectively, and should thus be allowable for at least the reasons described above with regard to claims 17 and 48. In addition, Koehler teaches that, when an expired item is replaced by the issuing authority, the systems remove the old item (col. 3, ll. 27-29). Koehler thus teaches away from that which is recited in claims 18 and 49. Therefore, Koehler does not anticipate claims 18 and 49. Withdrawal of the rejection of claims 18 and 49 is respectfully requested.

Claims 19 and 50 recite establishing a secure encrypted communications line with the user and transmitting the role certificate to the user. Claims 19 and 50 depend from claims 17 and 48, and should thus be allowable for at least the reasons described above with regard to claims 17 and 48. Additionally, as described above regarding claims 12 and 43, Koehler does not teach a secure encrypted communications line over which a role certificate is transmitted to a user, as recited in claims 19 and 50. Accordingly, Koehler does not anticipate claims 19 and 50. Withdrawal of the rejection of claims 19 and 50 is respectfully requested.

Claims 22 and 53 recite a method and computer program, respectively, of recovery of an expired role certificate associated with the role used for organizational encryption and as an organizational stamp...wherein a role member is an entity having a right to digitally sign organizational documents using the role certificate and decrypting information sent to members of the organization which has been encrypted using the role certificate. As described above with regard to claims 11 and 42, Koehler does not teach the use of a role certificate, and thus claims 22 and 53 should be allowable.

In addition, claims 22 and 53 recite transmitting a request to recover the expired role certificate along with a digital signature from each role member, listing all roles that the role member is listed as a role member on, and selecting the expired role certificate from the list of roles by the role member for recovery. The Office Action dated November 10, 2004, asserts that Koehler discloses transmitting of a digital signed certificate and discloses that the certificate has been encrypted and that decryption information is also known to receivers (pages 8 and 11). It is

respectfully submitted that this assertion does not properly address that which is recited in claims 22 and 53, in that the Office Action does not address transmitting a request to recover the expired role certificate along with a digital signature from each role member, as recited in claims 22 and 53. Nowhere does Koehler teach transmitting a request to recover the expired role certificate along with a digital signature from each role member. The Office Action dated November 10, 2004, further asserts that Koehler discloses a list that contains role members (at col. 3, ll. 11-13). This cited section describes a certificate revocation list that lists certificates which have been revoked and are no longer to be trusted (col. 3, ll. 11-13). This section describes a list of revoked certificates, and not roles that a role member is listed as a role member on, as recited in claims 22 and 53. It is further respectfully submitted that the Office Action dated November 10, 2004, does not address selecting the expired role certificate from the list of roles by the role member for recovery, as recited in claims 22 and 53, which is further not taught by Koehler. Koehler therefore does not anticipate claims 22 and 53. Withdrawal of the rejection of claim 22, as well as claims 23-25 which depend therefrom, and claim 53, as well as claims 54-56 which depend therefrom, is respectfully requested.

Amended claims 26 and 57 recite a method of revoking a role certificate and an associated role by a role administrator comprising transmitting a request to revoke the role certificate of a role member, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described above with regard to claims 11 and 42, Koehler does not teach the use of a role certificate, and thus amended claims 26 and 57 should be allowable.

In addition, amended claims 26 and 57 also recite transmitting a request to revoke the role certificate and the associated role by the role administrator for the role certificate along with a signature certificate for the role administrator, searching a database for all role certificates in which the role administrator is listed as a role administrator, and displaying to the role administrator all role certificates discovered. The Office Action dated November 10, 2004, (pages 8 and 11-12) asserts that Koehler discloses transmitting a request to revoke a role

certificate and the associated role (at col. 6, ll. 56-62). The cited section describes that a verification server checks if a certificate authority's certificate is authentic and rejects a client's request for verification if it is not (col. 6, ll. 56-62). Neither this cited section, nor any other section of Koehler, teaches transmitting a request to revoke the role certificate and the associated role by the role administrator for the role certificate along with a signature certificate for the role administrator, as recited in amended claims 26 and 57. The Office Action dated November 10, 2004, (pages 8 and 11-12) further asserts that Koehler discloses searching a database for all role certificates in which the role administrator is listed as a role administrator (at col. 8, ll. 28-31). Koehler teaches that a certificate revocation list is searched for digital certificates of users depending on a timestamp (col. 8, ll. 28-31), but does not teach searching a database for all role certificates in which the role administrator is listed as a role administrator, as recited in amended claims 26 and 57. The Office Action dated November 10, 2004, (pages 8 and 11-12) further asserts that Koehler discloses displaying to the role administrator all role certificates revoked (at col. 3, ll. 25-30). It is respectfully submitted that the Office Action dated November 10, 2004, has mischaracterized the language of amended claims 26 and 57, in that amended claims 26 and 57 recite displaying to the role administrator all role certificates "discovered," and not "revoked." Koehler does not teach a list of displaying to the role administrator all role certificates discovered, as recited in amended claims 26 and 57. Accordingly, amended claims 26 and 57 are not anticipated by Koehler. Withdrawal of the rejection of claim 26, as well as claims 27 and 28 which depend therefrom, and claim 57, as well as claims 58 and 59 which depend therefrom, is respectfully requested.

Claim 63 has been amended for clarity and recites a role certificate for organizational encryption and for use as an organizational stamp or seal comprising extensions having a plurality of bits which designate characteristics associated with the role certificate, wherein when a bit for encryption is set and a bit for signature is set, the role certificate may be used for both digital signatures and encryption, and a policy defining the limitations on valid usage of the role certificate. As described above regarding claim 11, Koehler does not teach the use of a role certificate. Also, as described above regarding claim 16, Koehler does not teach extensions

having a plurality of bits which designate characteristics associated with the role certificate, wherein when a bit for encryption is set and a bit for signature is set, the role certificate may be used for both digital signatures and encryption, and a policy defining the limitations on valid usage of the role certificate, as recited in claim 63. Koehler, therefore, does not anticipate claim 63. Withdrawal of the rejection of claim 63, as well as claims 64-66 which depend therefrom, is respectfully requested.

Claim 66 has been amended for clarity and recites that any time that the role certificate is used to sign on behalf of the organization, a signature certificate for the entity signing must be included. Koehler teaches that a certificate authority digital signature is used to verify the authenticity of an issued certificate (col. 5, ll. 17-20). However, Koehler does not teach that any time that the role certificate is used to sign on behalf of the organization, a signature certificate for the entity signing must be included, as recited in claim 66. Therefore, Koehler does not anticipate claim 66. Withdrawal of the rejection of claim 66 is respectfully requested.

For the reasons described above, claims 11-14, 16-22, 24, 26-28, 42-45, 48-53, 55, 57-59, and 63-66 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

IV. Rejection of Claims 29, 30, 60, and 61 Under 35 U.S.C. §102(e)

Claims 29, 30, 60, and 61 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,487,658 to Micali ("Micali"). Claims 29 and 60 have been amended. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Amended claims 29 and 60 recite a method and computer program, respectively, of recovering a former role and an associated role certificate by a role administrator comprising searching a database to determine if any role members associated with the role certificate are still in the organization, wherein each of the role members are members of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. Micali teaches an economical and efficient system for certificate revocation (Abstract). The system of certificate revocation taught by Micali is for

user digital certificates (see, *e.g.*, col. 2, ll. 21-51), and nowhere describes a role certificate as described in the present application. Micali, accordingly, does not contemplate the use of a role certificate, as recited in amended claims 29 and 60.

In addition, amended claims 29 and 60 further recite searching a database to determine if any role members associated with the role certificate are still in the organization, transmitting to at least one recovery agent a request for approval for the recovering of the role certificate when no role members are discovered to be in the organization, receiving approval from the at least one recovery agent for recovery of the role certificate, transmitting to the at least one recovery agent the role certificate retrieved when the recovery agent supplies an approval to recover the role certificate, and transmitting the role certificate to the role administrator by the recovery agent. The Office Action dated November 10, 2004, (pages 13 and 14) asserts that amended claims 29 and 60 are taught by Micali (at col. 25, ll. 20-34, and col. 24, line 67 through col. 25, line 6). These cited section teach that a user can access a tamper-proof directory on secure hardware to determine if any certificates on a list have been revoked, the user receiving a digitally signed answer from the secure hardware (col. 25, ll. 20-34), and that a "shopkeeper" may wish to verify the validity of a received certificate in a transaction by consulting a directory (col. 24, line 67 through col. 25, line 6). It is respectfully submitted that neither this cited section, nor any other section of Micali, teaches the recovery of a digital certificate, and that Micali does not teach any of searching a database to determine if any role members associated with the role certificate are still in the organization, transmitting to at least one recovery agent a request for approval for the recovering of the role certificate when no role members are discovered to be in the organization, receiving approval from the at least one recovery agent for recovery of the role certificate, transmitting to the at least one recovery agent the role certificate retrieved when the recovery agent supplies an approval to recover the role certificate, and transmitting the role certificate to the role administrator by the recovery agent, as recited in amended claims 29 and 60. Accordingly, Micali does not anticipate amended claims 29 and 60. Withdrawal of the rejection of claim 29, as well as claims 30 and 31 which depend therefrom, and claim 60, as well as claims 61 and 62 which depend therefrom, is respectfully requested.

Claims 30 and 61 recite that the at least one recovery agent is at least two recovery agents and both recovery agents must approve recovery before recovery of the role certificate occurs. Claim 30 depends from claim 29, and claim 61 depends from claim 60, respectively, and are thus allowable for at least the reasons described above with regard to claims 29 and 60. Additionally, Micali teaches that a list of revoked certificates, digitally signed by a certificate authority, can be provided to a user in the form of a message digitally signed by secure hardware (col. 25, ll. 37-49). However, this does not describe obtaining approval from two recovery agents to recover a certificate, and thus Micali does not teach two recovery agents approving recovery before recovery of the role certificate occurs, as recited in claims 30 and 61. Micali, therefore, does not anticipate claims 30 and 61. Withdrawal of the rejection of claims 30 and 61 is respectfully requested.

For the reasons described above, claims 29, 30, 60, and 61 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

V. Rejection of Claims 2-6, 10, 33-37, and 41 Under 35 U.S.C. §103(a)

Claims 2-6, 10, 33-37 and 41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Vaeth in view of U.S. Patent No. 6,275,859 to Wesley, et al. ("Wesley"). Claims 2, 10, 33, and 41 have been amended to correct typographical and grammatical errors. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 2, 10, 33, and 41 have been amended for clarity and recite that the role certificate comprises a public key, a private key, a signature algorithm ID, a validity period, extensions, and at least one policy. Wesley teaches a participation certificate obtained from a central authority by prospective members of a multicast session (Abstract). Wesley does not teach the use of a role certificate, such that the addition of Wesley does not cure the deficiencies of Vaeth to teach the recitations of claim 1 from which claim 2 depends, claim 7 from which claim 10 depends, claim 32 from which claim 33 depends, and claim 38 from which claim 41 depends. Additionally, Wesley teaches that a participation certificate includes starting and ending times for the period authorized by a node and identifies the role of the node in the multicast session,

such that it could be a repair node (col. 4, ll. 18-27). However, Wesley does not teach that a certificate (role certificate or otherwise) includes extensions and at least one policy, as recited in claims 2, 10, 33, and 41. Accordingly, the combination of Vaeth and Wesley does not teach or suggest claims 2, 10, 33, and 41. Withdrawal of the rejection of claim 2, as well as claims 3-6 which depend therefrom, claim 10, claim 33, as well as claims 34-37 which depends therefrom, and claim 41, is respectfully requested.

For the reasons described above, claims 2-6, 10, 33-37, and 41 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

VI. Rejection of Claims 15, 46, and 47 Under 35 U.S.C. §103(a)

Claims 15, 46, and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koehler in view of Vaeth. Claims 15, 46, and 47 have been amended to correct typographical and grammatical errors. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 15 and 46 have been amended for clarity and recite that the private key portion of the role certificate is stored in a key recovery authority for recovery in case of loss or expiration. The addition of Vaeth does not cure the deficiencies of Koehler to teach the recitations of claim 11 from which claim 15 depends, and claim 42 from which claim 46 depends. In addition, Vaeth teaches that a certificate request of a requester is stored at a certificate authority facility while the requester's certificate request is pending (col. 8, ll. 13-23). This section teaches that the requester does not yet have a certificate, and therefore does not yet have a private key that can be stored. Additionally, the certificate request storage is not for recovery in case of loss or expiration, as recited in claims 15 and 46, but is for awaiting approval or disapproval of the certificate request. Accordingly, the combination of Koehler and Vaeth does not teach or suggest claims 15 and 46. Withdrawal of the rejection of claims 15 and 46 is respectfully requested.

Claim 47 has been amended for clarity and recites that the role certificate comprises a public key, a private key, a signature algorithm ID, a validity period, extensions, and at least one policy. The addition of Vaeth does not cure the deficiencies of Koehler to teach the recitations

of claim 42, from which claim 47 indirectly depends. Additionally, for the reasons stated above with regard to claims 16, 21, 24, 28, 52, 55, and 59, the combination of Koehler and Vaeth does not teach or suggest claim 47. Withdrawal of the rejection of claim 47 is respectfully requested.

For the reasons described above, claims 15, 46, and 47 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

VII. Rejection of Claims 23, 25, 54, and 56 Under 35 U.S.C. §103(a)

Claims 23, 25, 54, and 56 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koehler in view of Wesley. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 23 and 54 recite authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority. The addition of Wesley does not cure the deficiencies of Koehler to teach the recitations of claims 22 and 53, from which claims 23 and 54 depend, respectively. In addition, Wesley teaches that a certificate authority verifies a certificate's authenticity with the certificate's public key before issuing a participation certificate (col. 4, ll. 3-6 and 15-17). The authentication taught by Wesley is to determine if a certificate is valid, and not to determine if a role member is either a member of a role or a role authority, as recited in claims 23 and 54. Also, Wesley teaches that the authentication is prior to issuing a participation certificate, and not before contacting a key recovery authority, as also recited in claims 23 and 54. Accordingly, the combination of Koehler and Wesley does not teach or suggest claims 23 and 54. Withdrawal of the rejection of claims 23 and 54 is respectfully requested.

Claims 25 and 56 recite that all members of the role are informed of the recovery of the role certificate. The addition of Wesley does not cure the deficiencies of Koehler to teach the recitations of claims 22 and 53, from which claims 25 and 56 depend, respectively. In addition, Wesley teaches that all nodes exchange their respective participation certificates as part of the multicast communication session (col. 4, ll. 39-44). However, this exchange of participation certificates is not informing all members of the recovery of a role certificate, as recited in claims

25 and 56. Therefore, the combination of Koehler and Wesley does not teach or suggest claims 25 and 56. Withdrawal of the rejection of claims 25 and 56 is respectfully requested.

For the reasons described above, claims 23, 25, 54, and 56 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

VIII. Rejection of Claims 31 and 62 Under 35 U.S.C. §103(a)

Claims 31 and 62 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Micali in view of Wesley. Claim 31 has been amended to correct a typographical error and claim 62 has been amended to change dependency based on the above described claim objection. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 31 and 62 have been amended for clarity and recite that both recovery agents must be authenticated as having authority to authorize the recovery of the role certificate prior to the role certificate being sent to the recovery agent. The addition of Wesley does not cure the deficiencies of Micali to teach the recitations of claims 29 and 60, from which claims 31 and 62 depend, respectively. In addition, Wesley teaches that a certificate authority verifies a certificate's authenticity with the certificate's public key before issuing a participation certificate (col. 4, ll. 3-6 and 15-17). The authentication taught by Wesley is to determine if a certificate is valid, and not to determine if recovery agents must be authenticated as having authority to authorize the recovery of a role certificate, as recited in claims 31 and 62. Also, Wesley teaches that the authentication is prior to issuing a participation certificate, and not prior to the role certificate being sent to the recovery agent, as also recited in claims 31 and 62. Therefore, the combination of Micali and Wesley does not teach or suggest claims 31 and 62. Withdrawal of the rejection of claims 31 and 62 is respectfully requested.

For the reasons described above, claims 31 and 62 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

Serial No. 09/690,544

Docket No. NG(MS)7178

CONCLUSION

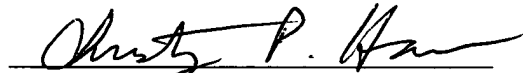
In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date

2/9/05



Christopher P. Harris

Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.

526 SUPERIOR AVENUE, SUITE 1111

CLEVELAND, OHIO 44114-1400

Phone: (216) 621-2234

Fax: (216) 621-4072